CLAIMS:

1. A method of determining the authenticity of a digital document sent by an unknown sender, the method comprising:

receiving a digital document, an encrypted digest of the document created by the sender using a hash algorithm, the digest being encrypted using a first token of the sender;

obtaining a second token relating to the first token;

decoding the encrypted digest using the second token;

using a hash algorithm to create a digest of the document; and

comparing the decrypted received digest with the newly created digest to determine the authenticity of the sender and the document.

2. A method according to Claim 1, wherein the receiving step comprises receiving a digital certificate of the sender.

3. A method according to Claim 2, wherein the obtaining step comprises the second token being sent as part of the sender's digital certificate.

4. A method according to Claim 2, further comprising carrying out an on-line check of the validity of the sender's certificate.

5. A method according to Claim 1, wherein the first and second tokens comprise private and public encryption/decryption keys of the sender.

6. A method according to Claim 1, further comprising printing out a copy of the document once the sender and the document have been authenticated.

7. A method according to Claim 6, wherein the method further comprises printing a verifying mark on the printed copy of the document to signify its authenticity.

8. A method according to Claim 1, wherein the transmitted document comprises a fax document.

9. A method of sending a digital document to a recipient together with data enabling the document and the sender to be authenticated, the method comprising:

creating a digest of the document using a hash algorithm;

encrypting the digest using a first token of the sender;

obtaining a second token relating to the first token of the sender, which can be used to decrypt the encrypted digest;

sending the encrypted digest, the digital document and the second token to the recipient.

10. A method according to Claim 9, wherein the transmitted document is a fax document.

11. A method according to Claim 9, further comprising the sender proving their identity prior to the sending step by transferring data from a personal portable data carrier holding the first token to a transmission station from which the document is to be sent.

12. A method according to Claim 11, wherein the proving step further comprises the sender entering a verifiable security identifier into the transmission station to establish that they are the legitimate owner of the portable data carrier.

13. A method according to Claim 11, wherein the step of encrypting the digest comprises supplying the digest of the document from the transmission station to the portable data carrier of the sender, encrypting the digest of the document on the portable data carrier, and returning the encrypted digest of the document from the portable data carrier to the transmission station.

14. A method according to Claim 9, further comprising obtaining details of the sender including the second token prior to transmitting the document.

15. A method according to Claim 14, wherein the step of obtaining details comprises obtaining the sender's details from a central database storing second tokens and other sender's details.

16. A method according to Claim 14, wherein the sender's details and the second token are provided in a sender's digital certificate.

17. A method according to Claim 9, wherein the first and second tokens comprise private and public encryption/decryption keys of the sender.

18. A device for determining the authenticity of a digital document sent by an unknown sender, the device comprising:

a communications module arranged to receive the document, an encrypted digest of the document created by the sender using a hash algorithm, the digest being encrypted using a first token of the sender, and a second token relating to the first token; and

a controller arranged to decode the encrypted digest using the second token; creating a digest of the document using a hash algorithm; and comparing the decrypted received digest with the newly created digest to determine the authenticity of the sender and the document.

19. A device for sending a digital document to a recipient together with data enabling the document and the sender to be authenticated, the device comprising:

a controller arranged to create a digest of the document using a hash algorithm and to encrypt the digest using a first token of the sender; and

a communications module arranged to obtain a second token related to the first token of the sender, which can be used to decrypt the encrypted digest and to send the encrypted digest, the digital document and the second token to the recipient.